

REMARKS

This Application has been carefully reviewed in light of the Office Action electronically mailed December 23, 2010. At the time of the Office Action, Claims 1-5, 7-10, 12-21, 23-26, 28-37, 39-42, and 44-60 were currently pending and stand rejected. Applicants respectfully request reconsideration and allowance of all pending claims.

Section 102 Rejections

The Office Action rejects Claims 1-5, 12-21, 27-31, 33-37, 44-48, 53, and 56-60 under 35 U.S.C. § 102(e) as being anticipated by U.S. Publication 2003/077394 to Dozortsev (“*Dozortsev*”). Applicants respectfully traverse these rejections.

Claims 1-55

Claim 1 recites moving the entry from the database of unfamiliar software to the database of known good software if it is determined that the entry has been in the database of unfamiliar software for a predetermined period of time. Claims 17 and 33 recite similar elements. The Office Action suggests that these elements are disclosed by various portions of *Dozortsev*. *See* Office Action, page 4. However, *Dozortsev* merely discloses a computer security system that identifies a potentially dangerous event on a client computer, identifies the executable code responsible for the event, uses a hash algorithm to generate a signature for the suspect executable code, and transmits the signature of the executable code to a central computer. *Dozortsev*, par. [0021]. The central computer then compares the received signature to a database of signatures to determine if the signature has already been identified in the database as “legitimate,” “malicious,” or “being investigated.” *Id.* at pars. [0022]-[0025], [0027]. If the signature does not match any entries in the database, then the executable code is transmitted from the client computer to the central computer for further investigation, which includes “in-house analysis of the executable code, called functions, executing the code in a sandbox environment, etc.” *Id.* at pars. [0022], [0040]. The client computer may request the status of the investigation from the central computer at predetermined time intervals. *Id.* at par. [0039]. Thus, these predetermined time intervals from *Dozortsev* are merely used by the client computer to obtain periodic updates regarding the status of the investigation, but the time intervals themselves are not relevant to the determination of whether the executable code is safe. The determination of whether the

executable code is safe is based on the investigation by the central computer, and this investigation *is not based on a predetermined period of time in which an entry has been in a database of unfamiliar software.* *Id.* at par. [0040]. Thus, *Dozortsev* fails to disclose moving the entry from the database of unfamiliar software to the database of known good software *if it is determined that the entry has been in the database of unfamiliar software for a predetermined period of time.*

Therefore, for at least these reasons, Applicants respectfully submit that Claims 1, 17, and 33 are allowable over the cited art used in the rejections and request that the rejections of these claims be withdrawn.

Claims 2-5, 6-10, 12-16, and 49-50 depend, either directly or indirectly, from Claim 1; Claims 18-21, 23-26, 28-32, and 51-53 depend, either directly or indirectly, from Claim 17; and Claims 34-37, 39-42, 44-48, and 54-55 depend, either directly or indirectly, from Claim 33. Thus, for at least the reasons discussed above with respect to Claims 1, 17, and 33, Applicants respectfully submit that Claims 2-5, 6-10, 12-16, 18-21, 23-26, 28-32, 34-37, 39-42, and 44-55 are allowable as depending from their allowable independent claims. Applicants respectfully request that the rejections of these claims be withdrawn.

Claims 56-60

Claim 56 recites a computer-implemented method for computer security, comprising:

determining, using the central processing unit, *quantitative information regarding the file for use in identifying whether the file should be added to a database of known good software,* the quantitative information selected from the group consisting of *a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed.*

The Office Action states that these claim elements are disclosed by paragraphs [0027], [0039], and [0040] of *Dozortsev*. See Office Action, page 7. However, as discussed above with respect to Claim 1, *Dozortsev* determines whether executable code is “legitimate” or “malicious” by comparison of a signature of the code to a database of signatures; and if the signature is not in the database, the executable code is sent to a central computer for further

investigation. *Dozortsev*, par. [0022]. The investigation includes activities such as in-house analysis of the executable code, called functions, and execution of the code in a sandbox environment. *Id.* at par. [0040]. As discussed above, the client computer in *Dozortsev* may request a status of the investigation at predetermined time intervals, but these time intervals are not relevant to the determination of whether the executable code is safe. *Id.* at par. [0039]. Thus, the investigation from *Dozortsev* **does not include determining any quantitative information for use in identifying whether to add a file to a database of known good software**. Moreover, because *Dozortsev* fails to disclose the use of any quantitative information for identifying whether to add a file to a database of known good software, it clearly does not disclose quantitative information for that purpose such as *a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed*. Thus, *Dozortsev* fails to disclose determining **quantitative information regarding the file for use in identifying whether the file should be added to a database of known good software**, the quantitative information selected from the group consisting of *a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed*.

Therefore, for at least these reasons, Applicants respectfully submit that Claim 56 is allowable over the cited art used in the rejection and request that the rejection of this claim be withdrawn.

Claims 57-60 depend, either directly or indirectly, from Claim 56. Thus, for at least the reasons discussed above with respect to Claim 56, Applicants respectfully submit that Claims 57-60 are allowable as depending from allowable independent Claim 56. Applicants respectfully request that the rejections of these claims be withdrawn.

Conclusion

Applicant has made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other apparent reasons, Applicant respectfully requests full allowance of all pending Claims. If the Examiner feels that a telephone conference or an interview would advance prosecution of this Application in any manner, the undersigned attorney for Applicant stands ready to conduct such a conference at the convenience of the Examiner.

Although Applicant believes no fee is due, the Commissioner is hereby authorized to charge any required fee or credit any overpayment to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,
BAKER BOTTS L.L.P.
Attorneys for Applicant



Chad C. Walters
Reg. No. 48,022
PHONE: (214) 953-6511

Date: April 25, 2011

CORRESPONDENCE ADDRESS:

Customer Number: **05073**